REMARKS

This paper is in response to the outstanding Office Action mailed on April 22, 2004, in the above-referenced application (August 22, 2004 being a Sunday). Upon entry of this Response, claims 1-13 and 16-25 are pending. Claims 14-15 are canceled. Claims 1 and 8 have been amended and claims 22-25 are newly added. No new matter has been introduced by the amendments. Entry and consideration of this Response and Amendment is respectfully requested.

Claim For Foreign Priority

Applicant respectfully requests that the Examiner acknowledge receipt of certified copies of the priority document No. GB 0021964.2 submitted on May 1, 2001. A copy of the postcard receipt evidencing the filing of the priority document with the Office is enclosed for Examiner's reference.

Response to Rejection Under 35 U.S.C. 103(a)

Claims 1-13 and 16-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sarpola et al. (U.S. Pat. No. 5,926,764, hereafter, "Sarpola") in view of Julius Caeser, and further in view of Brandman (US Pat. No. 5,974,144, hereafter "Brandman"), and further in view of Ala-Laurila et al. (U.S. Pat. No. 6,704,789). Applicant respectfully traverses the rejection for the following reasons.

The present invention, as presented in independent claims 1, 7, 8, and 20, provides an extremely powerful means for generating a volatile identification code for verifying a subscriber's identity and allowing access to, for example, a computer network, or for verifying an electronic transaction, such as a credit card transaction. The main basis of the present invention is the transmission by a host to the subscriber of a pseudorandom string, and the application by the subscriber of a mask code to the pseudorandom string so as to generate the volatile identification code. The volatile identification code is then transmitted back to the host, together with identification data identifying the subscriber. The host then uses the identification data to retrieve the subscriber's mask code from a secure database, applies the mask code to the pseudorandom string initially transmitted, and then compares the volatile identification code thus obtained (at the host) with the volatile identification code returned by the subscriber and checks to see if these match. If the volatile identification code obtained at the host matches the volatile identification code returned by the subscriber, then the subscriber's identity is verified.

Some prior art systems, including Great Britain patent number GB 2 279 541, which was submitted as part of an Information Disclosure Statement, utilize an overall architecture similar to that claimed. However, such prior art systems use computationally complex algorithms for applying a mask code to a pseudorandom string in order to generate a volatile identification code, and these algorithms must be applied by way of electronic computing means (e.g. hashing algorithms, public/private key encryption techniques, and the like). Other complex encryption algorithms of this type are described in Brandman, Puhl, Carter etc. on which the Examiner relies.

It is important to understand that these complex encryption algorithms cannot easily be applied, if at all, by a human user – they must be applied using electronic computing means. Although the present invention does not exclude the use of electronic computing means to assist in the application of the mask code to the pseudorandom string, this does not detract from the essential elegance and simplicity of the inventive technique.

A key inventive feature of the present invention is the provision of a simple mask code algorithm to generate a one-time volatile identification code, with the algorithm being applicable by a human user without difficulty. This is achieved by issuing a user with a fixed PIN code, which the user keeps secret, and which is additionally known only to the host. Where, for example, the PIN code (or mask code, as used in the application and claims) is 5269, the simple algorithm provided by the present invention is to select the 5th, 2nd, 6th and 9th characters from the pseudorandom string and to return these to the host as the volatile identification code. In this example, where the pseudorandom string is 1769405709, the mask code will return 4700 as the volatile identification code. In a subsequent transaction, using a different pseudorandom string, say 5689411785, the same mask code will return 4618 as the volatile identification code. It will be understood that the application of this algorithm is very easy for a human user without the need for computational assistance. Moreover, even if a fraudster were to come into possession of both a pseudorandom string and the volatile identification code, he would not be able unambiguously to derive the mask code due to redundancy in the pseudorandom string (i.e. repetition of numbers).

It is also to be emphasized that this methodology is not a Caesar cipher. The Caesar cipher works by shifting up or down the alphabet by a predetermined number of positions, this predetermined number being used for the entire message. However, this form of encryption is not easy for a human user to apply in his head without the aid of a written key, especially not when the shift is greater than 1 or 2. If a human user were, for example, conducting a credit card transaction in a store as described in the present application, receiving a pseudorandom string on his mobile phone, it would take him quite some time to perform a Caesar shift using his head, especially if his key was, for example "shift up 19 alphabetical positions". Even with the Caesar shift principle applied to numbers (e.g. with "shift up 5", 0 becomes 5, 1 becomes 6, 2 becomes 7, 5 becomes 0, 6 becomes 1 etc), this is still difficult and time consuming, because the user has to perform mental calculations. Moreover, the Caesar cipher is relatively easy to crack, simply by trying all of shifts 1 to 26 (for alphabetic), 1 to 10 (for numeric), or 1 to 36 (for alphanumeric).

A Vigenere cipher may be used as an improvement to the Caesar cipher. In a Vigenere cipher, a keyword is used as a basis for encryption, with each letter in the keyword indicating the number of characters by which a letter in the original message is to be shifted based on the position of the keyword letter in the alphabet. A Vigenere cipher also shifts different letters differently, based on the length of the keyword. As an example of a Vigenere cipher, if the keyword were "BAM", every third letter of the message starting at the first is shifted "B" (=1), every third letter starting at the second is shifted by "A" (=0) and every third letter starting at the third is shifted by "M" (=12). However, this is even more difficult for a human user to apply quickly and easily in his head, especially when under pressure such as at a supermarket checkout till.

The beauty of the present invention is that a human user can easily select characters from a pseudorandom string, such as, but not limited to, one displayed on his mobile telephone, a PIN pad at the supermarket, or the like, by selecting characters from the string on a positional basis using his mask code as described. He does not need to calculate individual Caesar shifts in his head, but merely selects the characters from the display without changing or shifting any of the characters themselves – he is merely selecting a subset of the characters and changing their positional order. In conclusion, the encryption methodology of the present invention is not a Caesar or Vigenere cipher, but something that is much more user-friendly while still remaining extremely secure. This methodology is clearly defined in independent claims 1, 7, 8 and 20 that do not read onto Caesar to Vigenere encryption techniques.

Claims 1 and 8

Claims 1 and 8 have been amended to remove the adjective "linear" in relation to the arrays. The support for the amendments can be found at page 5, line 29 to page 6, line 5 of the specification, which indicates that the arrays are only preferably linear, and the inventive technique could equally well be applied to a multi-dimensional dimensional array by using a mask code to select elements of the array in sequence on a positional basis defined by the elements of the mask code.

Sarpola describes a method for establishing a telecommunications connection. As correctly noted by the Examiner, part of the method (column 7, lines 22 to 56) includes an authentication step in which the host transmits an AUTHENTICATION_REQUEST message to a subscriber station and the subscriber station then returns an AUTHENTICATION_RESPONSE message. An optional ciphering function may be used when establishing connection to a local packet switched telephone network (PSTN) station. Sarpola is silent as to the nature of the AUTHENTICATION_REQUEST and AUTHENTICATION_RESPONSE messages, and gives no explanation whatsoever of any ciphering functions. There is no suggestion or teaching whatsoever in Sarpola that the messages are pseudorandom, as required by the claims of the present application. While the messages may well be numeric, alphabetical, or alphanumeric, it is most likely that the messages will be in binary numeric form. More importantly, Sarpola does not teach a pseudorandom message – indeed, the message is most likely to contain meaningful and ordered data and instructions intended to prompt the subscriber station to respond in the required manner.

The Examiner acknowledges that Sarpola does not teach the application of a mask code to a pseudorandom string so as to generate a volatile identification code in accordance with the rules set out in claims 1 and 8, but then asserts that this is known from the Caesar cipher. As discussed in some detail above, the encryption technique of claims 1 and 8 is not a Caesar cipher, nor is it a Vigenere cipher, but in fact is a completely different encoding technique with the important advantage of being easy for a human user to apply quickly and simply without having to apply mental effort. It is well established that, in order to show obviousness, all limitations must be taught or suggested by the prior art. In Re Boyka, 180 U.S.P.Q. 580, 490 F.2d 981 (CCPA 1974); MPEP § 2143.03. It is error to ignore specific limitations distinguishing over the references. In Re Boe, 184 U.S.P.Q. 38, 505 F.2d 1297 (CCPA 1974); In Re Saether, 181 U.S.P.Q. 36, 492 F.2d 849 (CCPA 1974); In Re Glass, 176 U.S.P.Q. 489, 472 F.2d 1388 (CCPA 1973). The mask code based encryption technique of the present invention is not taught or suggested by the prior art, and Applicant respectfully requests that the Examiner withdraw the rejection of Claims 1 and 8.

Likewise, the Brandman disclosure is also irrelevant, since it described the use of Caesar cipher and not the technique of claims 1 and 8. Brandman also requires powerful computing means to apply the Caesar cipher to broadband video signals, and does not in any way address the same issues as the present invention, which seeks to provide a powerful yet easy-to-use technique for generating a secure user identification code. It is well established that, in order to show obviousness, all limitations must be taught or suggested by the prior art. In Re Boyka, 180 U.S.P.Q. 580, 490 F.2d 981 (CCPA 1974); MPEP § 2143.03. It is error to ignore specific limitations distinguishing over the references. In Re Boe, 184 U.S.P.Q. 38, 505 F.2d 1297 (CCPA 1974); In Re Saether, 181 U.S.P.Q. 36, 492 F.2d 849 (CCPA 1974); In Re Glass, 176 U.S.P.Q. 489, 472 F.2d 1388 (CCPA 1973). The mask code based encryption technique of the present invention is not taught or suggested by the prior art, and Applicant respectfully requests that the Examiner withdraw the rejection of Claims 1 and 8.

Claims 1 and 8 are clearly distinguishable over the prior art of record. The Court of Appeals for the Federal Circuit has consistently held that where a claim is dependent upon a valid independent claim, the independent claim is *a fortiori* valid because it contains all the limitations of the independent claim plus further limitations. See, e.g., Hartness Intern. Inc. v. Simplimatic Engineering Co., 819 F.2d 1100, 1108 (Fed. Cir. 1987). Applicant reasserts the arguments above for each of claims 2-6, 9, 16-19, and 21 and asserts that these claims can be distinguished over the prior art at least for their dependency from independent claims 1 and 8. Applicant respectfully requests that the Examiner withdraw the rejection of these claims.

Claims 7 and 20

Independent claims 7 and 20 are directed to an embodiment in which the encryption technique is not explicitly defined, but in which the pseudorandom string contains at least one character that is representative of some condition of the data relating to the person. This may be, for instance, an indication of the balance of the person's bank account (see page 6, line 30 to page 7, line 18), this being indicated on a sliding scale from 0 to 9. For additional security, the person may be required to identify the position and/or meaning of the at least one representational character when responding to the host.

The Examiner references Ala-Laurila and argues that this feature is therein disclosed. However, column 7, lines 20 to 25 of Ala-Laurila merely states that "the HLR/VLR register uses the user ID to generate a random number RAND, a signed response SRES, and the ciphering key Kc, which are identified in the HLR/VLR register by the USER ID and replies by sending this information to the server." In other words, Ala-Laurila uses the USER ID as a seed for generating a pseudorandom number RAND, but there is no teaching that at least one special representative character is inserted into or included in RAND so as to represent a predetermined data condition. RAND does not include USER ID, but is merely selected from a list of pregenerated pseudorandom numbers on the basis of USER ID, as is well known in the art. SRES and Kc are not part of the random number RAND, but are separate data entities. It is well established that, in order to show obviousness, all limitations must be taught or suggested by the prior art. In Re Boyka, 180 U.S.P.Q. 580, 490 F.2d 981 (CCPA 1974); MPEP § 2143.03. It is error to ignore specific limitations distinguishing over the references. In Re Boe, 184 U.S.P.Q. 38, 505 F.2d 1297 (CCPA 1974); In Re Saether, 181 U.S.P.Q. 36, 492 F.2d 849 (CCPA 1974); In Re Glass, 176 U.S.P.Q. 489, 472 F.2d 1388 (CCPA 1973). Applicant respectfully asserts that the Examiner's argument that Ala-Laurila discloses the specific feature of claims 7 and 20 of the present application is without foundation, and asserts that the references cited neither teach nor suggest the subject matter of Claims 7 and 20. At least for the above reasons, claims 7 and 20 are clearly distinguished over the prior art of record. Therefore, Applicant respectfully requests that the Examiner withdraw his rejection of those claims.

Likewise, claims 10-13 are also distinguished over the prior art. The Court of Appeals for the Federal Circuit has consistently held that where a claim is dependent upon a valid independent claim, the independent claim is *a fortiori* valid because it contains all the limitations of the independent claim plus further limitations. See, e.g., Hartness Intern. Inc. v. Simplimatic Engineering Co., 819 F.2d 1100, 1108 (Fed. Cir. 1987). Applicant reasserts the arguments above for each of claims 10-13 and asserts that these claims can be distinguished over the prior art at least for their dependency from independent claim 7. Applicant respectfully requests that the Examiner withdraw the rejection of these claims.

Claims 22-25

Claims 22-25 are newly added to more specifically describe the claimed feature of the present invention. No new matter has been introduced. Claims 22-25 depend from independent claims 7 and 20 and are also believed to be distinguished over the prior art of record for at least the reasons set forth above with respect to claims 7 and 20.

CONCLUSION

In view of the foregoing, Applicant respectfully submits that all of the stated grounds of rejections and objections have been properly traversed or rendered moot. Thus, Applicant believes that the pending claims are in condition for allowance, and Notice to that effect is respectfully solicited. In the event that the Examiner is of the opinion that a brief telephone or personal interview will facilitate allowance of the application, he is courteously requested to contact Applicant's undersigned representative.

AUTHORIZATION

The Commissioner is authorized to charge the $55.00 fee for one-month extension of time and the $27.00 for addition of three dependent claims in excess of twenty to Deposit Account No. **50-0653.**

The Commissioner is also authorized to charge any additional fees associated with this filing, or credit any overpayment, to Deposit Account No. **50-0653.**

Respectfully submitted,

Date: August 23, 2004

By: ______________

James E. Goepel
Registration No. 50,851
Telephone No. (703) 903-7536
Facsimile No. (703) 749-1301
E-mail: goepelj@gtlaw.com

Correspondence Address
GREENBERG TRAURIG
1750 Tyson's Boulevard
Suite 1200
McLean, VA 22102

Customer No. 22191

Attorney Docket No.: A00291US (98148.12)
Applicant: Winston Donald Keech
Date: April 26, 2001
Serial No.: 09/663,281 Filed September 15, 2000
For:"Embedded Synchronous Random Disposable Code..."
Filing of: Information Disclosure Statement and Transmittal of Priority Document

Please acknowledge receipt of the above by date stamping and returning this card.

Very truly yours, P:\Seth\98148.12.pc.wpd
Seth M. Nehrbass